

METHOD FOR INSPECTING ON-VEHICLE CONTROL UNIT

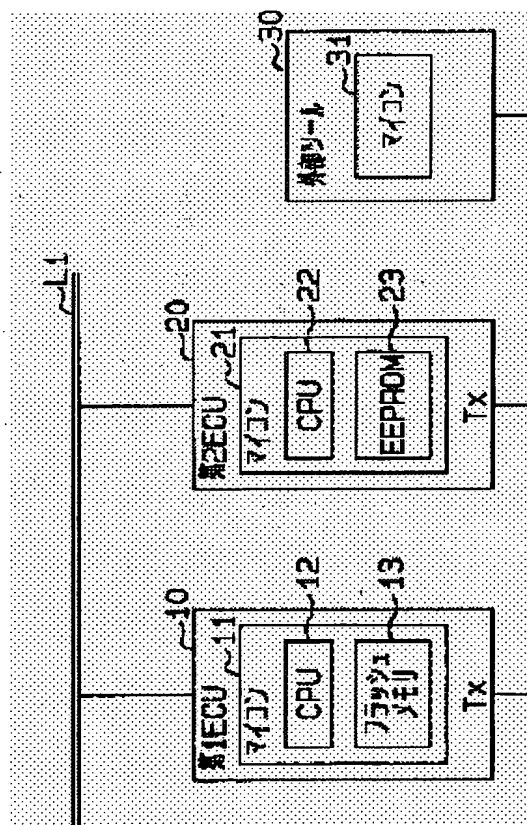
Patent number: JP2001202129
Publication date: 2001-07-27
Inventor: NAKAYAMA KIYONARI; KAMIYA KENJI
Applicant: DENSO CORP
Classification:
- international: G05B23/02; F02D45/00; G06F11/10; G06F12/16
- european:
Application number: JP20000012802 20000121
Priority number(s):

031356 U.S. PTO
10/759070
012004

Abstract of JP2001202129

PROBLEM TO BE SOLVED: To correctly inspect an on-vehicle control unit and to prevent the unit from being illegally modified.

SOLUTION: First and second ECUs 10, 20 are mutually connected so as to be communicated with each other through a multiplex communication line L1 and an external tool 30 is connected to respective ECUs 10, 20 through a serial communication line L2. In the decision of (inspecting) the corresponding/ falseness of the 1st ECU 10, the external tool 30 sends transmission data including a sum value calculation command to respective ECUs 10, 20 through the line L2. The 1st ECU 10 receives the sum value calculation command, calculates the sum value of data stored in a flash memory 13 and transmits the sum value to the 2nd ECU 20 through the line L1. The 2nd ECU 20 compares and decides the received sum value with a true sum value and transmits the decided result to the tool 30 through the line L2. Whether the 1st ECU 10 is a normal ECU or a false ECU is decided on the basis of the decision result.



THIS PAGE BLANK (USPTO)

(19) 日本特許庁 (J P) (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-202129

(P2001-202129A)

(43) 公開日 平成13年7月27日 (2001.7.27)

口開番号		P I		チコード(9桁)	
G05B 23/02	302	G05B 23/02	302K	3D026	
F02D 45/00	376	F02D 45/00	376P	3G084	
G06F 11/10	310	G06F 11/10	310B	5B001	
	320		320B	5B018	
B60R 15/02	665	B60R 15/02	665P	5H228	

(71) 出願人 株式会社デンソー

(72) 発明者 中山 聖也

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

(72) 発明者 社デンソー内

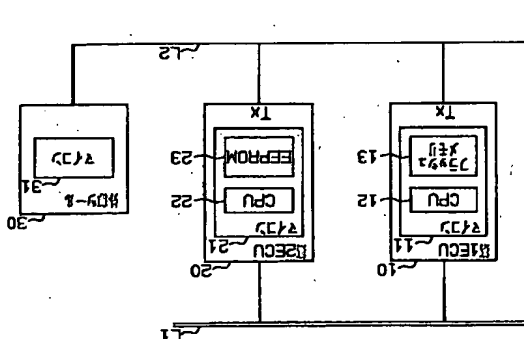
(72) 発明者 社デンソー内

(54) 発明の名称 車載制御ユニットの検査方法

(57) 要約

【発明】車載制御ユニットを正しく検査し、ひいては不正改造の防止を図る。

【解決手段】第1及び第2 ECU 10、20は多量通信線 L1 を介して相互に通信可能に接続され、外部ツール 30 はシリアル通信線 L2 を介して各 ECU 10、20 に接続されている。第1 ECU 10 の正誤判定 (検査) に際し、外部ツール 30 ではまず、サム値の算出指令を含む送信データをシリアル通信線 L2 を介して各 ECU 10、20 に送信する。第1 ECU 10 では、サム値算出指令を受けてフラッシュメモリ 13 内のデータのサム値を算出し、その後、そのサム値を多量通信線 L1 を介して第2 ECU 20 に送信する。第2 ECU 20 では、受信したサム値と真のサム値とを比較判定し、その判定結果をシリアル通信線 L2 を介して外部ツール 30 に送信する。この判定結果により、第1 ECU 10 が正規 ECU か偽 ECU が判断される。



【特許請求の範囲】

【請求項1】チェックサムのためとなるメモリを備える第1の制御ユニットと、それとは別の第2の制御ユニットとを備え、前記第1の制御ユニットのメモリについてデータのサム値を求め、該サム値により当該第1の制御ユニットを検査する車載制御ユニットの検査方法において、

サム値の算出指令を外部ツールから第1の制御ユニットへ送信する第1のステップと、

第1の制御ユニット内のメモリのサム値を算出し、該算出したサム値を第2の制御ユニットに送信する第2のステップと、

第2の制御ユニットにおいて受信したサム値を予め用意された真のサム値と比較し、その比較判定の結果から第1の制御ユニットを検査する第3のステップと、

前記検査結果を外部ツールに送信する第4のステップと、

【請求項2】第1の制御ユニット内のメモリは、電気的に書き換え可能な不揮発性メモリである請求項1に記載の車載制御ユニットの検査方法。

【請求項3】前記第2のステップでは、外部ツールが接続される通信線とは異なる別の通信経路を用いて、第1の制御ユニットから第2の制御ユニットへサム値を送信する請求項1又は2に記載の車載制御ユニットの検査方法。

【請求項4】外部ツールは、サム値算出指令の送信後、所定の応答待ち時間以内に受信した受信データを無効とする請求項1〜3の何れかに記載の車載制御ユニットの検査方法。

【請求項5】第2の制御ユニットは、外部ツールがサム値算出指令を送信した後、所定の制限時間以内に第1の制御ユニットからサム値が送信されない場合、当該第1の制御ユニットが不正である旨のコード情報を自身の不揮発性メモリに書き込む請求項1〜3の何れかに記載の車載制御ユニットの検査方法。

【請求項6】第1の制御ユニットが不正である旨が判定された状態で、第1の制御ユニットから外部ツールへのデータ送信が行われる場合、第2の制御ユニットは、第1の制御ユニットと外部ツールとを結ぶ通信線にデータミュータを送出する請求項1〜3の何れかに記載の車載制御ユニットの検査方法。

【請求項7】請求項6に記載の車載制御ユニットの検査方法において、

第2の制御ユニットは、データの送信ポートを物理ハイレベル又はローレベルに保持することでデータミュータを送出する車載制御ユニットの検査方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、車載制御ユニットの検査方法に関するものである。

【0002】

【従来の技術】この種の従来技術として、特開平1-132097号公報の「車両制御用メモリ書き換え装置」がある。同公報の装置は、外部ツールにより電気的に消去及び書き込み可能な制御メモリ (フラッシュメモリ) を搭載した ECU (車載制御ユニット) を備え、書き換え許可された時にのみ前記制御メモリに対するデータ書き換えが実施される。また、この装置は、制御メモリが配属するソフトウェア (制御プログラム) が正しいことを検査するものであり、その特徴として、

・予め配属しておいた制御メモリのサム値 (真値) と、ECU で算出したサム値とを共に表示し、それらと比較することによって正誤判定を行う。

・上記サム値の比較は外部ツールの内部で行い、その結果 (正偽) のみを返信する。

・イグニッションキースイッチの OFF から ON への切り換えにサム値の計算を行う。といった処理を実行する。

【0003】

【発明が解決しようとする課題】上記公報の従来技術では、ECU で計算したサム値を外部ツールに対してそのまま返信する。そのため、ECU と外部ツールとの通信データがモックすることになり、ECU が出力した正しいサム値を容易に知り得ることができ、ソフトウェアを書き換えなければならないものであるため、外部ツールに対して正しいサム値を常に返信するような不正なプログラムを不正改造者が作成し、それを ECU に組み込めば、正規のサム値算出アルゴリズムを知らなくとも容易に正規 ECU としてなりすますことが可能となる。これは、ECU 側で正誤判定を行う構成でも同様である。すなわち、モニタしたサム値を返信する偽プログラムを不正改造者が作成することにより、不正改造された ECU であっても、外部ツールは正しいサム値 (常に同じ) が返信されたと認識し、正しい ECU であると判断してしまう。

【0005】本発明は、上記問題に着目してなされたものであって、その目的とするところは、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることのできる車載制御ユニットの検査方法を提供することである。

【0006】

【課題を解決するための手段】請求項1に記載の車載制御ユニットの検査方法は、(1) サム値の算出指令を外部ツールから第1の制御ユニットへ送信する第1のステップ、(2) 第1の制御ユニット内のメモリのサム値を算出し、算出したサム値を第2の制御ユニットに送信する第2のステップ、(3) 第2の制御ユニットにおいて受信したサム値を予め用意された真のサム値と比較

し、その比較判定の結果から第1の制御ユニットを検査する第3のステップ、(4) 前記検査結果を外部ツールに送信する第4のステップ、といった各ステップを順に実施する。それ故、仮に正誤の制御ユニットが不正改造され、メモリ内の正しい値が外部ツール側に受信できるよう不正なプログラムが制御ユニットに組み込まれたとしても、第2の制御ユニットの改造又は置換を併せて実施しなければ、偽の制御ユニットが正規の制御ユニットとして取り扱われることはない、その結果、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる。

【0007】上記説明は特に、フラッシュメモリ等、電気的に書き換え可能な揮発性メモリにて第1の制御ユニット内のメモリが構成される場合に有効である（請求項2）。

【0008】請求項3に記載の発明では、前記第2のステップにおいて、外部ツールが接続される通信線とは異なる別の通信経路を用いて、第1の制御ユニットから第2の制御ユニットへサム値を送信する。本発明によれば、第1の制御ユニットから発信されるサム値の算出結果が外部ツールで受信されることがないため、外部ツール側で本来必要でないデータが受信され、それが原因で処理が遅延するといった不都合が回避される。

【0009】請求項4に記載の発明では、外部ツールは、サム値算出指令の送信後、所定の応答待ち時間以内に受信した受信データを検知する。つまり、外部ツールがサム値算出指令を送信すると、当該外部ツールは本来、上記第2～第4の各ステップが実施される処理時間を経た後、サム値算出指令に応答するデータを受信する。こうした実状でも拘らず、サム値算出指令の後、直ぐに外部ツールがデータを受信した場合、制御ユニットが不正改造された可能性が高い。それ故、規定に満たない時間で受信したデータを無効化すると共に、制御ユニットが不正改造された旨を判断する。

【0010】請求項5に記載の発明では、第2の制御ユニットは、外部ツールがサム値算出指令を送信した後、所定の制限時間以内で第1の制御ユニットからサム値が送信されない場合、当該第1の制御ユニットが不正である旨のコーンプレックス自身（第2の制御ユニット内）の不揮発性メモリに書き込む。かかる場合にも、制御ユニットが不正改造されたことが判定でき、更にその旨を不揮発性メモリに格納することにより、後々の異常診断に役立てることができる。なお、不揮発性メモリに書き込まれたコーンプレックスは、外部ツールからの要求に従い第2の制御ユニットから外部ツールに送信される良い。

【0011】ところで、第2の制御ユニットにより第1の制御ユニットを検査し、その結果を外部ツールに送信する上記構成では、第1の制御ユニットが不正改造されていても、不正改造された当の制御ユニットが自身を正確なECUであるとする偽データを送信すると、外部ツール

は不正改造された制御ユニットを正確なものとして判断するおそれがある。

【0012】そこで、請求項6に記載の発明では、第1の制御ユニットが不正である旨が判定された状態で、第1の制御ユニットから外部ツールのデータ送信が行われる場合、第2の制御ユニットは、第1の制御ユニットと外部ツールとを結ぶ通信線にダイミュータを送出する。これにより、不正改造された制御ユニットから外部ツールへ向け偽データが送出したとしても、ダイミュータで前記偽データが破壊（無効化）される。従って、不正改造された制御ユニットを外部ツールが正確なものと判断するといった不都合が解消される。

【0013】特に、請求項7に記載のように、第2の制御ユニットは、データの送信ポートを制御ハイレベル又はローレベルに保持することでダイミュータを送出すると良く、これにより簡易構成での実装が可能となる。

【0014】
【発明の実施の形態】（第1の実施の形態）この発明を具体化した本発明の形態では、エンジン制御等を見るECUにて車載制御ユニットを構成し、このECUに対して外部ツールを接続し、当該ECUの検査やデータの交換等を行うこととしている。以下、その詳細を図面に従って説明する。

【0015】図1は、制御システムの構成を示すブロック図である。本システムでは、第1の制御ユニットとしての第2ECU20とを備える。この第1及び第2ECU20は、20は、多量通信線L1を介して相互に通信可能に接続されている。第1ECU10は、燃料噴射制御や点火時期制御等、エンジン系の主要な制御を受け持つECUであり、その内部のマイコン21は、各種制御の中核をなすCPU12、電気的に消去及び書き込み可能なフラッシュメモリ13、その他図示しないRAMや入出力回路等を備える。

【0016】また、第2ECU20は、エアパス制御やABS制御等、補助的な制御を受け持つECUであり、その内部のマイコン21は、各種制御の中核をなすCPU22、電源変動時にも記憶内容を保持するEEPROM23、その他図示しないRAMや入出力回路等を備える。

【0017】外部ツール30も同様に、CPU、メモリ、入出力回路等からなる周知のマイコン31を備える。この外部ツール30は、第1ECU10の正誤判定等の検査や、第2ECU10内のフラッシュメモリ13のデータを検出し、シリアル通信線L2を介して第1及び第2ECU10、20と接続される。これにより、第1及び第2ECU10、20が外部ツール30との間でシリアル通信によるデータのやり取りが行われる。

【0018】第1ECU10の正誤判定（検査）の概要

を、図2を用いて説明する。かかる場合、フラッシュメモリ13内のデータのサム値と既知の正しいサム値とが比較され、両者が一致すれば、第1ECU10が正規なものであると判断される。なお図2では、処理順序を表すため、(1)～(5)の連続番号を付している。

【0019】先ず始めに、サム値の算出指令を送信するデータをシリアル通信線L2を介して外部ツール30から第2ECU20に送信する（図の(1)）。第1ECU10側では、サム値算出指令を受けてフラッシュメモリ13内のデータのサム値Xsumを算出し（図の(2)）、その後、そのサム値Xsumを多量通信線L1を介して、すなわち外部ツール30が接続されるシリアル通信線L2とは異なる別の通信経路を介して、第2ECU20に送信する（図の(3)）。

【0020】第2ECU20では、受信したサム値Xsumと、予め登録されている真のサム値Xrefとを比較判定し、その判定結果をシリアル通信線L2を介して外部ツール30に送信する（図の(4)）。また、この第2ECU20では、サム値不一致の場合に第1ECU10が不正改造されたことを意味するダイミュータを配送する。

【0021】そして、前記判定結果がサム値の一致（Xsum=Xref）を示すものであれば、外部ツール30において第1ECU10が正規ECUであると判断し、前記判定結果がサム値の不一致（Xsum≠Xref）を示すものであれば、外部ツール30において第1ECU10が偽ECUであると判断する。

【0022】以下では、外部ツール30による第1ECU10の正誤判定に際し、各ECU10、20及び外部ツール30内の各マイコン11、21、31により実施される処理の流れを図3及び図4のフローチャートに従って説明する。始めに、外部ツール30の処理の流れを図3のフローチャートで説明する。

【0023】例えば修理工場等において作業者が外部ツール30を操作すること図3の処理がスタートし、先ずステップ101では、コマン送信処理によりサム値算出指令を各ECU10、20に送信する。また、ステップ102ではタイマセットを行う。このステップ101、102が通信前処理に相当する。

【0024】その後、この外部ツール30では、コマン送信に対する第2ECU20からの受信確認を行う。すなわち、タイマがリセットしていないことを条件に（ステップ103が「NO」）、ステップ104では、前記ステップ101のコンマ送信に対する応答を第2ECU20から受信したか否かを判断する。

【0025】応答が無いままタイマがリセットした場合（ステップ103が「YES」）、そのままステップ107に進む。ステップ107では、通信異常に関するダイミュータを取り出し、その後、ECU異常の旨を判断する。なお、ステップ103が「YES」の場合、ステップ101

に戻り、コマン送信を再度実施しても良い。この場合、コマン再送信の回数を予め制限しておき、例えばタイマがリセットが3回繰り返されたら、通信異常であると判断してステップ107に進む構成としても良い。

【0026】コマン送信に対する応答を第2ECU20から受信すると、ステップ105に進み、その受信データに含まれるサム値の判定結果を取り出す。そして、その判定結果がサム値一致に該当するものである、ステップ106を肯定判定し、ECU正常である旨を判断する。また、前記判定結果がサム値不一致に該当するものである、ステップ106を否定判定し、ステップ107でダイミュータを取り出し、その後、ECU異常の旨を判断する。

【0027】次に、第1及び第2ECU10、20の処理の流れを図4のフローチャートに従って説明する。ここで、図4(a)は第1ECU側10の処理を示し、図4(b)は第2ECU20側の処理を示す。先ず、図4(a)に従い、第1ECU10側の処理の流れを説明する。

【0028】第1ECU10内のマイコン11は、先ずステップ201において、外部ツール30よりコマンを受信したか否かを判断し、YESであればステップ202に進み、算出式 $Xsum = \sum Data(i)$ により、サム値Xsumを算出する。すなわち、フラッシュメモリ13内の規定されたアドレス領域についてアドレスのデータを全て加算し、その和をサム値Xsumとする。その後、ステップ203では、前記算出したサム値Xsumを多量通信線L1を介して第2ECU20に送信し、本処理を一息終了する。

【0029】一方、第2ECU20内のマイコン21は、図4(b)のステップ301において、第1ECU10よりサム値Xsumを含むデータを受信したか否かを判断し、YESであればステップ302に進み、受信データからサム値Xsum（生データ）を取り出す。

【0030】その後、ステップ303では、予め登録されている真のサム値Xrefを取り出し、続くステップ304では、サム値Xsum（生データ）と真のサム値Xrefとを比較する。

【0031】両サム値が一致すれば、そのままステップ306に進み、サム値の比較結果をシリアル通信線L2を介して外部ツール30に対して送信する。この場合、前記図3の処理では、ECU正常である旨が判断される。

【0032】また、両サム値が不一致であれば、ステップ305で第1ECU10が不正改造されたことを意味するダイミュータをEEPROM23に登録した後、ステップ306でサム値の比較結果をシリアル通信線L2を介して外部ツール30に対して送信する。この場合、外部ツール30による前記図3の処理では、EEP

ROM23に登録したダイアグコードが取り出されると共に、ECU異常である旨が判断される。

【0033】なお本実施の形態では、図3のステップ101の処理が本発明の「第1のステップ」に、図4(a)のステップ202、203の処理が「第2のステップ」に、図4(b)のステップ304の処理が「第3のステップ」に、図4(b)のステップ306の処理が「第4のステップ」に、それぞれ該当する。

【0034】以上述べた本実施の形態によれば、以下に示す効果が得られる。つまり、上記ECUの検査方法によれば、仮に第1ECU10(正規のECU)が不正に改造され、フラッシュメモリ13の正しいサム値(算出したサム値Xsum)を外側ツール30側に送信できるような不正なプログラムがECUに組み込まれたとしても、第2ECU20の改造又は置換を併せて実施しなければ、偽のECUが正規のECUとしてなりすますことができない。その結果、第1ECU10を正しく検査し、ひいては不正改造の防止を図ることができ、

【0035】また、外側ツール30が接続されるシリアル通信線L2とは異なる別の通信経路(多重通信線L1)を用いて、第1ECU10から第2ECU20へサム値Xsumを送信するので、サム値Xsumが外側ツール30側で受信されることはない。それ故、外側ツール30側で本来必要でないデータが受信され、それが原因で処理が煩雑するといった不都合が回避される。

【0036】(第2実施の形態) 次に、本発明における第2実施の形態を説明する。但し、本実施の形態では、上述した第1実施の形態と即時であるものは説明を省略し、第1実施の形態との相違点を中心に説明する。

【0037】上記第1実施の形態では、第2ECU20でサム値の比較判定が行われ、その判定結果のみがシリアル通信線L2を介して外側ツール30に送信されるため、この第2ECU20の代わりに正規ECUである偽データを送信するシリアル通信線L2に流すことで、偽のECUが正規ECUになりすますことが考えられる。すなわち、図5に示すように、第1ECU10(正規ECU)の代わりに偽ECU40が組み込まれた場合、偽ECU40自身が「正規ECU」である旨の偽データをシリアル通信線L2を介して外側ツール30に送信すると、外側ツール30は偽ECU40が正規のものであると誤判定するおそれがある。

【0038】そこで、その対策として本実施の形態では、第1ECU10が不正である旨が判定された場合に、第2ECU20よりシリアル通信線L2にダイミデータを送出し、偽ECUが「正規ECU」である旨の偽データが送信されることを妨害する。以下、第2ECU20並びに外側ツール30による監視機能について、詳しく説明する。

【0039】本実施の形態において、外側ツール30

は、前記図3の処理に代えて図6の処理を実施し、第2ECU20は、前記図4(b)の処理に代えて図7の処理を実施する。但し、各図において変更の無い処理は同じステップ数を付すと共に、重複する説明を簡略化する。なお、第1ECU10の処理は前記図4(a)をそのまま適用するため、図示及び説明は省略する。

【0040】図6において、外側ツール30は、ステップ101、102で通信前処理を行い、その後、ステップ103、104で第2ECU20からの受信履歴を確認し、このとき、タイムアウトしておらず且つ、コマンド送信に対する応答を第2ECU20から正常に受信すると、ステップ401に進む。

【0041】ステップ401では、コマンド送信(サム値算出指令)から所定の応答待ち時間T1が経過したか否かを判断する。この応答待ち時間T1は、コマンド送信の後、各ECU10、20で行われる処理の所要時間を考慮して設定される時間であり、本発明は応答データを受信する旨の無い時間である。但し、このT1は勿論、受信タイムアウトを判定する時間よりも短い時間である。

【0042】データを正常に受信した時に所定の応答待ち時間T1が経過していれば、第2ECU20からの受信データが正規データであるとみなし、後続のステップ105に進み、そして、受信データ内に含まれるサム値の判定結果により、第1ECU10が正常か異常かを判断する(ステップ105~107)。

【0043】また、応答待ち時間T1前にデータ受信し場合は、受信データが偽データであるとみなして当該データを無効とする。そして、直ぐにステップ107に進み、ダイアグコードの取り出し、第1ECU10の異常判定を行う。

【0044】つまり、サム値算出指令の後、応答待ち時間T1を待たずに直ぐに外側ツール30がデータを受信した場合、第1ECU10が不正改造された可能性が高いと図える。それ故、規定に満たない時間で受信したデータを無効化する。

【0045】一方、図7において、第2ECU20は、外側ツール30からのコマンド受信の旨を判断すると、ステップ501からステップ502に進み、タイムセツトを行う。

【0046】その後、コマンド受信からの経過時間が所定の制限時間T2以内であることを条件に(ステップ503がNO)、ステップ504では、外側ツール30からのコマンド送信(サム値算出指令)に反応して第1ECU10からサム値を受信したか否かを判断する。

【0047】こうした受信履歴の処理において、第1ECU10からサム値を受信できない場合、コマンド受信からの経過時間が制限時間T2を超える場合(ステップ503がYES)、ステップ508に進み、異常ダイアグコードをEEPROM23に登録する。すなわちこの

場合、第1ECU10が偽ECUであることとみなし、不正改造が行われたことを意味するダイアグコードを第2ECU20内のEEPROM23に登録する。

【0048】また、制限時間T2以内にサム値を受信すると、後続のステップ505に進み、ステップ505~507では、受信データに含まれるサム値Xsumと、登録済みの真のサム値Xrefとを取り出すと共に、それら両サム値を比較する。そして、両サム値が一致すれば、ステップ511に進み、サム値の比較結果(この場合は正常判定の結果)を外側ツール30に対して送信する。

【0049】また、両サム値が不一致であれば、ステップ508で異常ダイアグコードをEEPROM23に登録した後、ステップ509に進み、ステップ509では、所定の受信有効時間T3(ステップ510がYESの期間)内においてECU異常時ににおける通信線モニタ処理を実施する。なお、受信有効時間T3とは、外側ツール30が受信データを有効とする時間であって、シリアル通信線L2上の偽データを、外側ツール30が正規データとしてとり違える可能性がある時間帯に該当する。

【0050】通信線モニタ処理に際し、第2ECU20は図8の処理を実施する。すなわち、シリアル通信線L2をモニタし、第1ECU10から外側ツール30に対して送信されるコマンドがあるかどうかを判断する(ステップ601)。そして、コマンド送信が確認されると、シリアル通信線L2上のコマンドを無効化すべく、送信ポートTxからダイミデータを送出する(ステップ602)。なお、簡易構成を実現する上では、送信ポートTxを論理レベル又はローレベルに保持することでダイミデータを送出すと良い。

【0051】通信線モニタ処理をT3期間内で継続した後、ステップ511では、サム値の比較結果(この場合は異常判定の結果)を外側ツール30に対して送信し、その後本処理を一旦終了する。

【0052】ここで、通信線モニタ処理について、図9のタイムチャートを参照しより具体的に説明する。つまり、第1ECU10が偽ECUに置換され、その偽ECUの送信ポートTxから図示のような偽データが送信される場合、第2ECU20は、自身の送信ポートTxを論理ローレベルに保持する。この場合、外側ツール30では、シリアル通信線L2を介して受信されるデータに関しては、ストップビットを検出できないことからエラー発生であると判定され、結果的に受信データが無効化されることとなる。これにより、偽ECUが正規ECUであるようになりすますことが防止できる。

【0053】なお本実施の形態では、上記第1実施の形態との違いとして、図7のステップ507の処理が「第3のステップ」に、図7のステップ511の処理が「第4のステップ」に、それぞれ該当する。

【0054】以上第2実施の形態によれば、上記第1実施の形態における効果に加え、以下の特徴的な効果を奏する。

(イ) 外側ツール30は、サム値算出指令の送信後、所定の応答待ち時間T1以内に受信した受信データを無効とするので、第1ECU10が不正改造された旨が好適に判断できる。

【0055】(ロ) サム値算出指令の後、所定の制限時間T2以内に第1ECU10からサム値が送信されない場合、第2ECU20は第1ECU10が不正改造されたこととみなし、その旨のダイアグコードをEEPROM23に登録するので、異常判定の履歴が記憶保持できる。また、外側ツール30からの要求に応じてダイアグコードを取り出すことにより、後々の異常診断に役立てることができる。

【0056】(ハ) 第1ECU10が不正改造された旨が判定された状態で、第1ECU10から外側ツール30へのデータ送信が行われる場合、第2ECU20はシリアル通信線L2にダイミデータを送出するので、不正改造されたECUから外側ツール30へ向けて偽データが送られてくとしても、ダイミデータで前記偽データが検出(無効化)される。従って、不正改造されたECUを外側ツール30が正規なものとして判断するといった不都合が解消される。

【0057】なお本発明は、上記以外に次の形態にて具体化できる。上記各実施の形態では、第1の制御ユニットとして、燃料噴射制御や点火時期制御等、エンジンの主要な制御を受け持つ第1ECU10を假し、第2の制御ユニットとして、エアパージ制御やABS制御等、補助的な制御を受け持つ第2ECU20を假したが、その構成は任意で良い。要は、少なくとも2つのECU(制御ユニット)を備え、検査対象ではない方のECUによりサム値の比較判定を行う構成であれば良い。

【0058】上記各実施の形態では、第1及び第2ECU10、20を多重通信線L1で接続すると共に、外側ツール30と各ECU10、20とをシリアル通信線L2で接続したが、この通信システムの構成を適宜変更しても良い。要は、サム値算出指令及びサム値比較結果が外側ツール30で受信される通信経路と、サム値の算出結果が送信される通信経路とが別々に設けられる構成であればよい。

【図面の簡単な説明】

【図1】発明の実施の形態における制御システムの概略構成を示すブロック図。

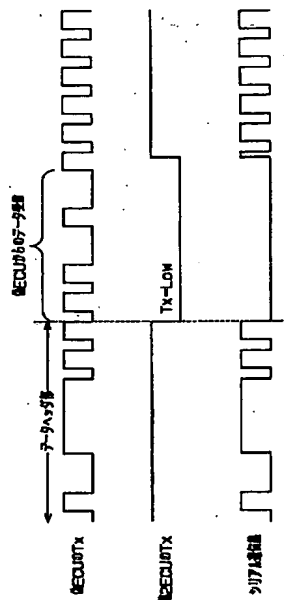
【図2】ECUの正体判定の様子を示す説明図。

【図3】外側ツールの処理の流れを示すフローチャート。

【図4】第1ECU及び第2ECUの処理の流れを示すフローチャート。

【図5】第2実施の形態の説明のための概略図。

【図9】



フロントページの続き

(51)Int.Cl.⁷ B60S 5/00 F I B60S 5/00 9A001

Fターム(参考) 3D026 BA22 BA28 3G084 BA00 DA32 EB06 EB22 5B001 AA14 AB01 AC01 AD03 AE01 5B018 GA03 GA06 GA10 HA13 HA31 JA26 LA12 NA06 RA11 RA12 5E223 AA10 CC08 DD03 EE11 EE19 9A001 EB03 EE34 JJ77 LL06

THIS PAGE BLANK (USPTO)